

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 2001-069480
 (43)Date of publication of application: 16.03.2001

(51)Int.Cl.

H04N 7/167
 H04H 1/00
 H04H 1/02
 H04L 9/08

(21)Application number: 11-243918

(71)Applicant: MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing: 30.08.1999

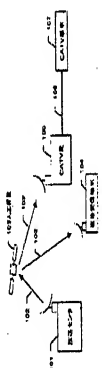
(72)Inventor: NAGATA MINEHISA
 KITA TERUHIRO
 SAKURAI ATSUNORI
 NAITO YASUFUMI
 GOTO YOSHIMASA

(54) CONDITIONAL ACCESS SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a conditional access system where a repeater relays contents sent from a broadcast center without descrambling the contents with a simple configuration and the repeater can uniquely manage conditional access of a terminal.

SOLUTION: A broadcast center 101 transmits a 1st EMM together with contents, a 1st ECM including a same scramble key Ks, and a 2nd ECM, and a CATV station 105 multiplexes a 2nd EMM on a transport stream including the contents to relay the resulting stream to a CATV channel 106. A CATV terminal 107 discriminates viewing on the basis of the 2nd ECM and the 2nd EMM, extracts the key Ks and views the contents, then the CATV station 107 relays the contents with a simple configuration without the need for descrambling the contents and manages conditional access of the CATV terminal 107.



* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] A center apparatus, one or more repeating installation, and the first one or more terminal units are connected in the first transmission line. Said repeating installation and the second one or more terminal units are the conditional access systems connected, and in the second transmission line said center apparatus. Carry out the scramble of the contents containing either an image, a sound or data, and it sends out to said first transmission line. Encipher the first common information including the first access area judging that performs an access judging to a scramble key which carries out the scramble of said contents, and said contents, and it carries out multiplex to said contents. While enciphering the first individual information including contract information of the first work key that enciphers said first common information, and said first terminal unit and carrying out multiplex to said contents. Encipher the second common information including the second access area judging that performs an access judging to said scramble key and said contents with the second work key, and it carries out multiplex to information which enciphers the second individual information containing said contents which received from said first transmission line to said second transmission line. Carry out multiplex to information which enciphers the second individual information including contract information of said second work key and said second terminal unit, and contains said contents, and it sends out to said second transmission line. Said first terminal unit on a basis the first access area judging contained in said first common information, and contract information included in said first individual information said second terminal unit. A conditional access system characterized by performing access control to said contents based on the second access area judging contained in said second common information, and contract information included in said second individual information.

[Claim 2] A center apparatus, one or more repeating installation, and the first one or more terminal units are connected in the first transmission line. Said repeating installation and the second one or more terminal units are connected in the second transmission line. Further, said center apparatus and said repeating installation are conditional access systems connected, and in the third transmission line said center apparatus. Carry out the scramble of the contents containing either an image, a sound or data, and it sends out to said first transmission line. Encipher the first common information including the first access area judging that performs an access judging to a scramble key which carries out the scramble of said contents, and said contents, and it carries out multiplex to said contents. While enciphering the first individual information including contract information of the first work key that enciphers said first common information, and said first terminal unit, carrying out multiplex to said contents and sending out to said first transmission line. Encipher the second common information including the second access area judging that performs an access judging to said scramble key and said contents with the second work key, and it sends out to said third transmission line. While relaying information containing said contents which received from said first transmission line to said second transmission line, said repeating installation said second common information received from said third transmission line. Carry out multiplex to information which carries out multiplex to information containing said contents, enciphers the second individual information including contract information of said second work key and said second terminal unit, and contains said contents, and it sends out to said second transmission line. Said first terminal unit on a basis the first access area judging contained in said first common information, and contract information included in said first individual information said second terminal unit. A conditional access system performing access control to said contents based on the second access area judging contained in said second common information, and contract information included in said second individual information.

[Claim 3] Whenever it changes said center apparatus, send it out once, and said second common information said repeating installation. The conditional access system according to claim 1 or 2 characterized by repeating and sending out said second common information with a constant interval until it will receive the second common information changed into the next, if said second common information is received.

[Claim 4] The conditional access system according to any one of claims 1 to 3, wherein said center apparatus enciphers said second common information with a cipher system other than a cipher system of said first common information.

[Claim 5] The conditional access system according to any one of claims 1 to 4, wherein said repeating installation enciphers said second individual information with a cipher system other than a cipher system of said first individual information that said center apparatus performs.

[Claim 6] The conditional access system according to any one of claims 1 to 5, wherein said first access area judging of said first common information, and describing the second access area judging of said second common information by a channel bit map.

[Claim 7] The conditional access system according to any one of claims 1 to 5, wherein said first access area judging of said first common information, and describing the second access area judging of said second common information by a channel bit map.

[Claim 8] The conditional access system according to any one of claims 1 to 7, wherein said center apparatus stores and sends out said scramble key to said second common information, and said repeating installation receives said second common information and adds and sends out an access area judging.

[Claim 9] Said center apparatus stores said scramble key in said second common information, enciphers and sends it out with said second work key, and said repeating installation, while the third work key enciphers and sends out a field including said second common information that received said second common information, added an access area judging and was received, and said added access area judging. The conditional access system according to any one of claims 1 to 7 storing and sending out said second work key and said third work key to said second individual information.

[Claim 10] The conditional access system according to any one of claims 1 to 9, wherein said repeating installation removes and relays said first common information that exists in information containing said contents which received from said first transmission line.

[Claim 11] The conditional access system according to any one of claims 2 to 9, wherein said repeating installation replaces and relays said first common information that exists in information containing said contents which received from said first transmission line, and said second common information received from said third transmission line.

[Claim 12] Said center apparatus carries out multiplex [of the empty information] to said contents suitably, sends it out to said first transmission line, and said repeating installation, from said first transmission line, remove said first individual information and information containing said contents which received is relayed. The conditional access system according to any one of claims 1 to 11 replacing and carrying out multiplex [of information and said second individual information of said empty which exists in information containing said contents].

[Claim 13] The conditional access system according to any one of claims 1 to 11, wherein said repeating installation replaces and carries out multiplex [of said first individual information that exists in information containing said contents which received from said first transmission line, and said second individual information].

[Claim 14] The conditional access system according to any one of claims 1 to 11, wherein said repeating installation carries out frequency multiplexing of said second individual information to a frequency band other than a frequency band from which information containing said contents is relayed and sends it out to it.

[Claim 15] Said repeating installation and said second terminal unit are connected even in fourth transmission line where said second transmission line is another, and said repeating installation,

Relay information containing said contents to said second transmission line, send out said second individual information to said fourth transmission line, and to it said second terminal unit. The conditional access system according to any one of claims 1 to 11 performing access control to said contents based on the second received common information and the second individual information received from said fourth transmission line from said second transmission line.

[Claim 16] In said second common information, said contents provide a program attribute which shows the Tia program or a pay-per-view program, and to it it said center apparatus, Store, send out the Tia information and pay-per-view information to the second access area judging in said second common information, and said repeating installation, responding to employment — said program attribute of said second common information — either the Tia program or a pay-per-view program — or. The conditional access system according to any one of claims 1 to 15, wherein it changes into a value which shows both and said second terminal unit judges access control by Tia, pay-per-view either, or both with reference to said program attribute.

[Claim 17] The conditional access system according to any one of claims 1 to 16 sending said second work key to said repeating installation with a storage from said center apparatus.

[Claim 18] The conditional access system according to any one of claims 1 to 16 transmitting said second work key to said repeating installation from said center apparatus in the first transmission line.

[Claim 19] The conditional access system according to any one of claims 1 to 16 transmitting said second work key to said repeating installation from said center apparatus in the third transmission line.

[Claim 20] The conditional access system according to any one of claims 1 to 16 transmitting said second work key to said repeating installation using a public network from said center apparatus.

[Claim 21] The conditional access system according to any one of claims 16 to 20, wherein it sends said second work key to said center apparatus with a storage from said one certain repeating installation and said center apparatus sends said second received work key to said other repeating installation.

[Claim 22] Two-way communication is possible for said first transmission line, and said second work key is transmitted to said center apparatus from said one certain repeating installation in said first transmission line. The conditional access system according to any one of claims 16 to 20, wherein said center apparatus sends said second received work key to said other repeating installation.

[Claim 23] Two-way communication is possible for said third transmission line, and said second work key is transmitted to said center apparatus from said one certain repeating installation in said third transmission line. The conditional access system according to any one of claims 16 to 20, wherein said center apparatus sends said second received work key to said other repeating installation.

[Claim 24] The conditional access system according to any one of claims 16 to 20, wherein it transmits said second work key to said center apparatus using a public network from said one certain repeating installation and said center apparatus sends said second received work key to said other repeating installation.

[Claim 25] The conditional access system according to any one of claims 17 to 24, wherein said center apparatus or said repeating installation enciphers and transmits said second work key using a private key cryptosystem.

[Claim 26] The conditional access system according to any one of claims 17 to 24, wherein said center apparatus or said repeating installation enciphers and transmits said second work key using a public-key cryptosystem.

[Claim 27] Store, send out said center apparatus to said second common information if needed, and a telephone number of the first viewing history collection place said repeating installation. The conditional access system according to any one of claims 1 to 22, wherein it stores and sends out a telephone number of the second viewing history collection place to said second individual information if needed and said terminal unit transmits a viewing history, using preferentially a

telephone number of said first viewing history collection place.

[Claim 28] A common information stripper which is a common information stripper belonging to the conditional access system according to claim 1 or 2, and is characterized by said common information stripper removing said first common information from information which is installed in said repeating installation and contains said contents.

[Claim 29] Said first common information of information containing said contents which it is a common information multiplexer belonging to the conditional access system according to claim 2, and said common information multiplexer was installed in said repeating installation, and received from said first transmission line. A common information multiplexer replacing said second common information received from said third transmission line.

[Claim 30] An individual information stripper which is an individual information stripper belonging to the conditional access system according to claim 1 or 2, and is characterized by said individual information stripper removing said first individual information from information which is installed in said repeating installation and contains said contents.

[Claim 31] An individual information multiplexer which is an individual information multiplexer belonging to the conditional access system according to claim 1 or 2, and is characterized by said individual information multiplexer replacing said first individual information in information which is installed in said repeating installation and contains said contents, and said second individual information.

[Claim 32] A common information multiplexer which is a common information multiplexer belonging to the conditional access system according to claim 3, and is characterized by sending out said common information multiplexer repeatedly until it receives the second common information changed into the next in said second common information it was installed in said repeating installation and received.

[Translation done.]

* NOTICES *

JPO and WIPI are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the limited reception method for performing the reception control of a terminal unit to the signal which relayed signals, such as satellite broadcasting, via the transmission line of CATV etc., or a system.

[0002]

[Description of the Prior Art] Generally in satellite broadcasting etc., the passthrough method etc. are known as a method of transmitting the signal by which scramble was carried out as it is, without performing descrambling and re-scramble by a CATV station etc., and performing limited reception. [0003] The method of SAIMARU crypto is known as a method of making two or more limited

reception intermingled to one contents.

[0004] Hereafter, a Prior art is explained using figures.

[0005] Drawing 40 is a figure showing the important section of the system configuration of a passthrough method.

[0006] CATV station 4009 is connected with the satellite center 4001 by the satellite connection using the satellite 4008, and the terminal unit 4015 is connected with CATV station 4009 with the CATV network. * NOTICES *

JPO and WIPI are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. **** shows the word which can not be translated.

3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The entire configuration figure of the conditional access system in a 1st embodiment of this invention.

[Drawing 2] The internal configuration figure of the broadcast center in a 1st embodiment of this invention.

[Drawing 3] The internal configuration figure of the CATV station in a 1st embodiment of this invention.

[Drawing 4] The internal configuration figure of the direct reception terminal in a 1st embodiment of this invention.

[Drawing 5] The internal configuration figure of the CATV terminal in a 1st embodiment of this invention.

[Drawing 6] The basic constitution figure of EMM in a 1st embodiment of this invention.

[Drawing 7] The basic constitution figure of ECM in a 1st embodiment of this invention.

[Drawing 8] The figure showing operation of the limited reception module in a 1st embodiment of this invention.

[Drawing 9] The lineblock diagram of the viewing-and-listening judging TIA bit in a 1st embodiment of this invention.

[Drawing 10] The lineblock diagram of the contract information TIA bit in a 1st embodiment of this invention.

[Drawing 11] The lineblock diagram of the viewing-and-listening judging bit map in a 1st embodiment of this invention.

[Drawing 12] The lineblock diagram of the contract information bit map in a 1st embodiment of this invention.

[Drawing 13] The internal configuration figure of the multiplex section in a 2nd embodiment of this invention.

[Drawing 14] The figure showing the important section of the header unit of an MPEG 2 transport stream packet.

[Drawing 15] The basic constitution figure of ECM in a 2nd embodiment of this invention.

[Drawing 16] The internal configuration figure of the multiplex section in a 3rd embodiment of this invention.

[Drawing 17] The basic constitution figure of EMM in a 3rd embodiment of this invention.

[Drawing 18] The figure showing operation of the multiplexer in a 3rd embodiment of this invention.

[Drawing 19] The internal configuration figure of the multiplex section in a 4th embodiment of this invention.
 [Drawing 20] The figure showing operation of the individual information multiplexer in a 4th embodiment of this invention.
 [Drawing 21] The internal configuration figure of the multiplex section in a 5th embodiment of this invention.
 [Drawing 22] The figure showing operation of the common information multiplexer in a 5th embodiment of this invention.
 [Drawing 23] The lineblock diagram of the second ECM in a 5th embodiment of this invention.
 [Drawing 24] The lineblock diagram of the second ECM in a 6th embodiment of this invention.
 [Drawing 25] The lineblock diagram of the second ECM in a 8th embodiment of this invention.
 [Drawing 26] The lineblock diagram of the second EMM in a 8th embodiment of this invention.
 [Drawing 27] The internal configuration figure of the CATV station in a 7th embodiment of this invention.
 [Drawing 28] The figure showing the frequency band on the CATV circuit in a 7th embodiment of this invention.
 [Drawing 29] The internal configuration figure of the CATV terminal in a 7th embodiment of this invention.
 [Drawing 30] The internal configuration figure of the CATV station in an 8th embodiment of this invention.
 [Drawing 31] The internal configuration figure of the CATV terminal in an 8th embodiment of this invention.
 [Drawing 32] The internal configuration figure of the broadcast center in a 9th embodiment of this invention.
 [Drawing 33] The inside of the multiplex section of the CATV station in a 9th embodiment of this invention, and a surrounding lineblock diagram.
 [Drawing 34] The figure showing operation of the common information multiplexer in a 9th embodiment of this invention.
 [Drawing 35] The entire configuration figure of the conditional access system in a 10th embodiment of this invention.
 [Drawing 36] The figure showing operation of the CATV terminal in a 10th embodiment of this invention.
 [Drawing 37] The entire configuration figure of the conditional access system in a 11th embodiment of this invention.
 [Drawing 38] The internal configuration figure of the broadcast center in a 11th embodiment of this invention.
 [Drawing 39] The internal configuration figure of the second CATV station in an 11th embodiment of this invention.
 [Drawing 40] The figure explaining the conventional passthrough method.
 [Drawing 41] It is a figure explaining the conventional SAIMARU crypto method.
 [Description of Notations]
 101, 3701 broadcast centers
 104 and 3702 Direct reception terminal
 105 CATV station
 107 CATV terminal
 202 and 3803 First EMM generation part
 204 and 3804 First ECM generation part
 205, 3202, and 3806 Second ECM generation part
 206, 3201, and 3805 Second Kw Management Department
 207, 3203, and 3808 SAIMARU crypto control section

303, 2703, a 3903 PSI converter
 304 and 3904 Multiplex section
 305, 2704, a 3905 QAM modulation part
 306, 2705, and 3908 Frequency conversion part
 307, 2706, and 3001 Second Kw Management Department
 308, 2707, and 3002 Second EMM generation part
 404, 504, 2904, and 3104 Separation part
 405, 505, 2905, and 3105 Limited reception module
 1301 Common information stripper
 1302, 1602, 2102, and 3302 Multiplexer
 1501 ECM identifier
 1601 Individual information stripper
 1701 EMM identifier
 1901 Individual information multiplexer
 2101 and 3301 Common information multiplexer
 2301 Program attribute
 2710 Modulation part
 2708 Frequency conversion part
 2901 Distribution part
 2909 The second EMM extraction part
 3003 Communications department
 3101 Communications department
 3204 Communications department
 3303 Communications department
 3501 The first viewing history collection center
 3502 The second viewing history collection center
 3703 The first CATV station
 3705 The first CATV terminal
 3706 The second CATV station
 3708 The second CATV terminal
 3907 Nth Kw Management Department
 3908 The Nth EMM generation part

[Translation done.]

* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

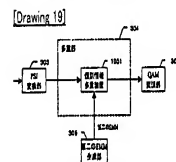
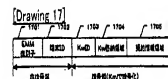
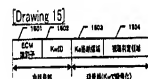
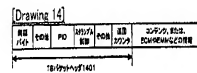
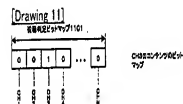
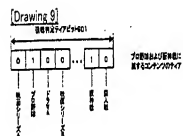
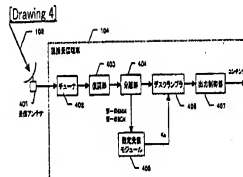
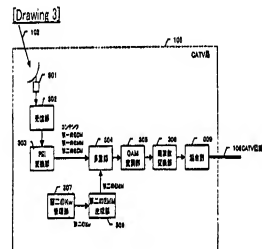
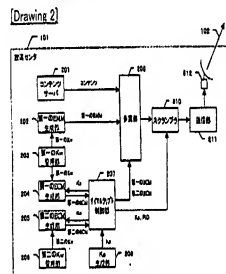
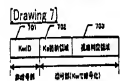
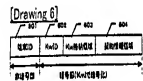
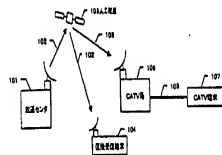
1. This document has been translated by computer. So the translation may not reflect the original precisely.

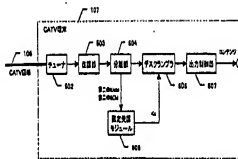
2. **** shows the word which can not be translated.

3. In the drawings, any words are not translated.

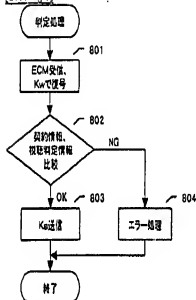
DRAWINGS

[Drawing 1]

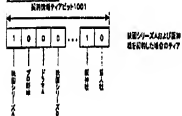




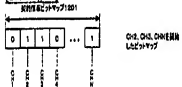
[Drawing 8]



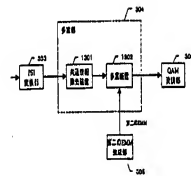
[Drawing 10]



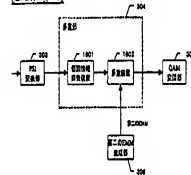
[Drawing 12]



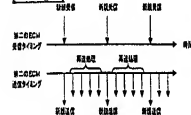
[Drawing 13]



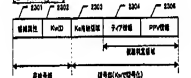
[Drawing 16]



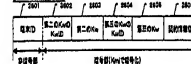
[Drawing 22]



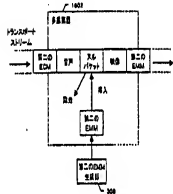
[Drawing 23]



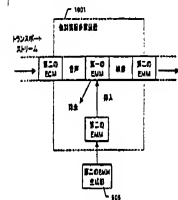
[Drawing 26]



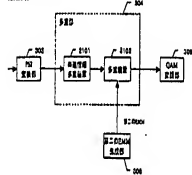
[Drawing 18]



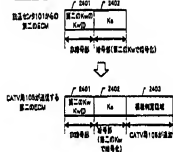
[Drawing 20]



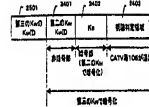
[Drawing 21]



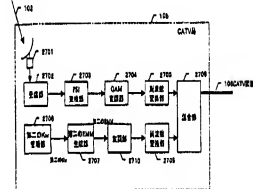
[Drawing 24]



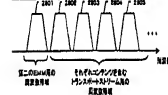
[Drawing 25]



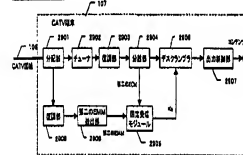
[Drawing 27]



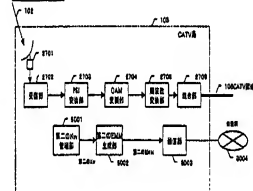
[Drawing 28]



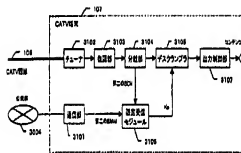
[Drawing 29]



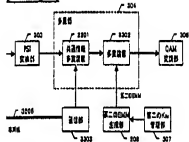
[Drawing 30]



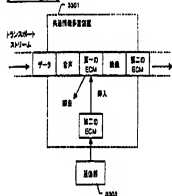
[Drawing 31]



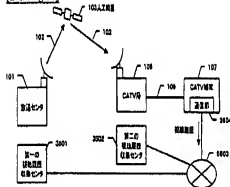
[Drawing 33]



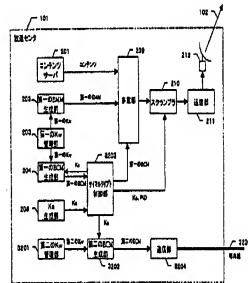
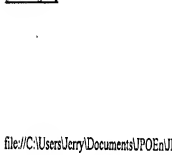
[Drawing 34]



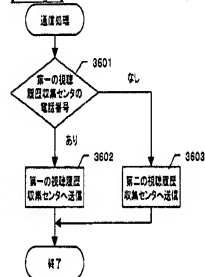
[Drawing 35]



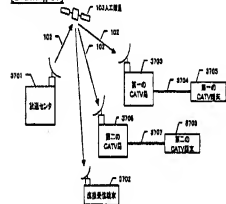
[Drawing 36]



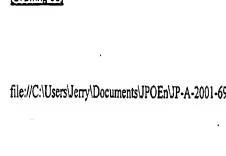
[Drawing 38]

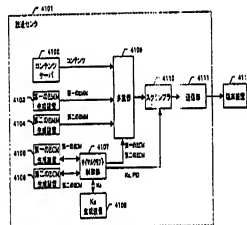
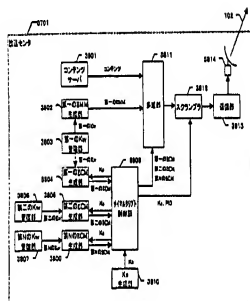


[Drawing 39]



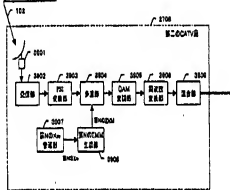
[Drawing 40]



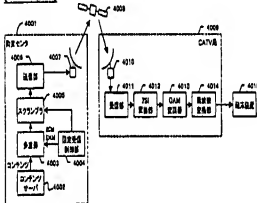


[Translation done.]

[Drawing 39]



[Drawing 40]



[Drawing 41]

る。PS1変換部402では、番組別付情報(PS1)の一部であり、変調周波数などの伝送路の情報とコンテンツとを関連付ける情報を伝送するためのNITを、衛星伝送用途からケーブル伝送用途に変換してQAM変換部403へ送信し、QAM変換部403はCATVで規定されているQAM方式に変換して周波数変換部404へ送信し、周波数変換部404はストリームをCATVの伝送周波数に変換してCATVへ送出する。

【0012】端末装置40は、CATV網からストリームを受信し、自分のEMMを復号し、契約情報及びKwを保持し、スクランブルされたコンテンツを脱暗する場合には、まず、該コンテンツに付随するECMを受信してKwで復号し、ECM内の判定領域と契約情報とを比較し脱暗許可の有無を調べる。脱暗許可が有りと判定されれば、ECM内のKsを用いて該コンテンツをデスクランブルすることができ、脱暗可能となる。

【0013】以上のように、パススルー方式においては、CATV局4009では単にストリームをCATV網に送った変調方式などに交換するのみであり、ECMやEMMを復号する必要もなく、その内容には関与せずに送出される。

の中継することとなる。この方式では、各端末装置との契約管理は全て拠点センタ4003が行う。

【0014】また、図41は、同一のコンテンツに対して複数の限定受信を課金させるサイマルクリプト方式のシステム構成の要部を示す図である。図41において、コンテンツ、ECM、EMMなどの関係は上記で説明したのと同様である。

【0015】装置センタ404は、第一の既定受発信方式に
 属する端末装置に対するEEMを生成する第一のEEM
 生成装置405と、第二の既定受発信方式に属する端末装
 置に対するEEMを生成する第二のEEM生成装置406と、
 第一の既定受発信方式のECMを生成する第一のEC
 M生成装置405と、第二の既定受発信方式のECMを生成
 する第二のECM生成装置406と、映像や音などにて構
 成されるデータを読み出すコンテンツサーバ407と、
 コンテンツを第一及び第二のEEM並びにECMと
 を多量する多量部408と、コンテンツをスクランブルす
 るためのKsを一定周期にて生成するKs生成装置409
 と、第一及び第二のECMを多重するMUX部410と、

Dとk sとをスクランブルした出力するサイマルクリプト装置c07と、スクランブルを復元するスクランブラi02と、ストリームを逐次処理して端末装置c12に送出する送信部i03とを備えている。

【0010】このシステムの放送センター41では、コンテンツサーバ42が録音や音声などから生成されるコンテンツを多数c09へ送信する。第一のEMM生成装置c01は、第一の放送装置43を通じて各端末装置c12に対して、コンテンツへの識別情報を与える契約情報領域を含む第一のEMMを多数c09へ送信し、第二のEMM生成装置c02、第二の放送装置44を通じて各端末装置c12へ、第二のEMMを多数c10へ送信する。

図11に対して以上と異なる二つのEMMの取得可否を与える契約構成を生成する二つのEMMを多量に作成し、送受信する。また、Kを生成するc08コンテキストから抽出するためのKを一定回数で生成し、サイマルクリプト制御部c04へ送受信する。サイマルクリプト制御部c04は、受信したKを第一のECM生成装置c05及びc10に渡し、第一のECM生成装置c05は、コンテキストに対する照会操作を決定する。この決定結果と受信したKとを組合せ第一のECMを生成し、サイマルクリプト制御部c04へ送受信し、第二のECM生成装置c10は、上記と同一のコンテキストKに対する照会操作を決定する。この決定結果と受信したKとを組合せ第二のECMを生成し、サイマルクリプト制御部c04へ送受信する。

10117) サイクル第二の多量第420は、受信した第一のECM及び第二のECMを多量第420に送信するとともに、スクランブルをコンテンプクに適用するP IDとKsとをスクランブル4210に送信する。多量第420は、コンテンプク、第一のECM、第二のECM、第一のECM及び第二のECMを多重化した一つのストリームとしてスクランブル4210を行い、スクランブル4210は、指定されたPIDとKsとを基に、該当するコンテンプクに対してスクランブルを行い、送信部4211へ送達する。送信部4211は、このストリームに伝送路に適合した変調処理を行い、この変調処理を送出する。

【0018】第一の既定受渡方式に属する受渡書412は、ストリーミングを含む第一のEEMを受渡し、契約前情報と保持し、コンテンツに付随する第一のEEMの特定情報と契約情報とを比較し、視聴許可が有りと判定されれば該コンテンツのデータストリームを行うことができる既定受渡となる。また、第二の既定受渡方式に属する既定受渡413は、ストリーミングを含む第二のEEMを受渡し、契約前情報と保持し、コンテンツに付随する第二のEEMの特定情報と契約情報とを比較し、視聴許可が有りと判定されれば該コンテンツのデータストリームを行うことができる既定受渡となる。

【0018】このように、サイマルクリプト方式を用いれば、同一のコンテンツに対して複数の限定受信を混在させることが可能となる。

【0020】さらに、上記で説明したバスカー方式とサイクリック方式とを組み合わせると簡単に数値的な限定変位が可能な。すなわち、図40における数値的な限定変位の40に1に対して任意な定変位40に1を同一と見なすと、第2センタ401において複数の限定変位を混在させることが可能となり、CATVやHDTVではこれを用いたECM、EVMには関係せずにと用いる。たとえば、図41は、コンパニオンチャンネル4011から衛星回線を通して直接受信するような直接受信端末がある場合に、直接受信端末には同一の限定変位方式を利用し、CATVやHDTVの受信機では限定変位方式が異なる

の限定受信方式を利用するC
mとCATV局4009は独立し
償を実現することが可能とな

【0021】
【発明が解決しようとする課題】
従来の技術を組み合わせた方
すべき端末装置に対するEM
れる第二のEM生成装置の
には、CATV局が管理する
EMMそのものをCATV
必要があるため、型枠構造

る。
[0022]また、システム
端末装置を管理するCAT
のこの場合には、装置
MMの伝送容量が大幅に増
30Mbpsである。第二
ることは、コンテンツの伝
ることで、コンテンツの伝
などといった影響が及ぼす
に第二のEMMの伝送容量
にに影響は及ばなくなる
れたことで第二のMM全
が増え、各地装置間の負荷
り、顧客が利用したいコン

【0023】本発明は、こ
あり、センタ装置からのコ
において、コンテツプをデ
また、ECMやEMMを復
デツプに影響を及ぼさず
行うことができる限定受信
のシステムを構成する装置
いる。

(0024)

【課題を解決するための手段】
 図1及び図2は、本発明の第1の実施形態に係る装置の構成を示すブロック図である。図1は、第1の伝送路と第2の伝送路とを接続するための装置の構成を示す。図2は、第1の伝送路と第2の伝送路とを接続するための装置の構成を示す。

5. 仮定のコンテンツを含む情報と第二の伝送路に接続するとともに、第二のワーク領域及び第二のコンテンツ契約情報を含む第二の識別情報とを符号化したコンテンツを含む情報と多重して第二の伝送路へ送し出し、第一の端末装置は、第一の識別情報に含まれるアクセス判定情報と第一の識別情報に含まれる契約情報とを基に、第二の端末装置は、第二の識別情報と含まれるアクセス判定情報と第二の識別情報に含まれる契約情報とを基にコンテンツへのアクセス制御を行うという手段を有している。

[0025] 以上のように第1の発明では、センタ装置

がコンテンツ及び第一の個別情報とともに、コンテンツをスクランブルしたスクランブル鍵を第一の共通情報及び第二の共通情報を含めて送出し、中継装置は受信したコンテンツ、第一の個別情報、第一の共通情報及び第二の共通情報を受信するごとく中継するとともに、第二の個別情報を復号して送出するようとしたので、中継装置に接続された第二の端末装置に対して、センタ装置からのコンテンツを簡単な構成で伝送でき低コストで受信されるとともに、中継装置独自の放送受発を行うことがで

【0026】第2の発明は、センタ装置と1つ以上の中
継装置及び1つ以上の第一の端末装置とが第一の伝送路
で接続され、中継装置と1つ以上の第二の端末装置とが
第二の伝送路で接続され、センタ装置と中継装置とはさ
らに第三の伝送路で接続される原定受信システムであ
る。センタ装置は、映像、音声またはデータなどのい

れを含むコンテンツをスクランブルして第一の伝送路へ送出し、コンテンツをスクランブルするスクランブル鍵及びコンテンツへのアクセス判定を行う第一のアクセス判定領域を含む第一の共通情報域を符号化してコンテンツに多量し、第一の共通情報域を符号化する第一のワーク鍵及び第一の端末装置の契約情報を含む第一の管理情報域を符号化してコンテンツに多量して第一の伝送路へ送出するとともに、スクランブル鍵及びコンテンツへのア

システム実行作業のアクセス情報抽出を第三の伝送路へ通信し、中継装置は、第一の伝送路から第二の伝送路へのアクセスを含む情報を第二の伝送路に送り出すとともに、第三の伝送路から受信した第二の共通情報部、コンテンツを含む情報を第三、第四のワーク領域及び第一の端末装置の実行情報を含む第二の監視情報と等号化してコンテンツを含む情報を第三の伝送路へ送り出し、第一の端末装置は、第一の共通情報部と第二の監視情報と第一のアクセス情報と第一の個別情報に含まれる実行情報とを基に、第二の端末装置は、第二の共通情報部と第二の監視情報と第一のアクセス情報と第二の個別情報に含まれる実行情報とを基にコンテンツのアクセス制御を行うという手段を有している。

(c) 図 10 のように、本発明の他の実施形態として、本発

(9)

15

[0082]以上より第2の2の説明では、第二ワーク群である1つの中間装置からセンタ制御へ記憶体送り、更にセンタ制御から他のワーク群をその中間装置に送り出すようにして、簡単に他のワーク群と共有でき、中間装置が主幹的役割のワーク群の変更を行うことができるという効果が得られる。

[0083]第2の2の説明では、第一の送信機は方向通信可能であり、第二のワーク群をもとめて中間装置からセンタ制御へ第一の送信機で伝送し、中間装置が実行された第二のワーク群をその他の中間装置へ送るといって第2のワーク群を用いる。以上より第2の2の説明では、第2のワーク群である1つの中間装置がセンタ制御へ第一の送信機にて伝送し、センタ制御が他のワーク群をその他の中間装置へ送るとともに別の、任意のタイミングで第二のワーク群を変更でき、即時に共有でき、中間装置が主幹的役割のワーク群の変更を行うことができるという効果が得られる。

(1084) 第23の発明では、第三の伝送路は双方向通信路であって、第二のワーク段にある一つのセンタ装置へ第三の伝送路を通じて伝送し、センタ装置は受け取った第三の伝送路からの信号の中程位置の信号を有している。以上のように第23の発明では、第二のワーク段にある一つのセンタ装置からセンタ装置へ第三の伝送路を通じて伝送し、センタ装置は受け取った第三の伝送路からの信号の中程位置の信号を有している。以上のように第23の発明では、第二のワーク段を要する、即時に共有できる、中程位置が本発明の第二のワーク段の変更を行なうことができる。

【0085】第24の発明では、第二のワーク図をある1つの中間装置からセンタ装置へ公衆網を用いて伝送し、センタ装置は受け取った第二のワーク図をその他の中間装置へ送るといった手段を有している。

【0068】以上のように第24の発明では、第二の

用いて伝送し、センタ装置は第二のワーク値をその他の中継装置へ送るようにしたので、任意のタイミングで第二のワーク値を変更でき、即時に共有でき、中継装置も主体的に第二のワーク値の変更を行うことができるといふ効果が得られる。

【0087】第25の発明では、センタ装置または中間装置は、第二のワーク鍵を秘密鍵暗号方式を用いて暗号化を行い、伝送するという手段を有している。

【0068】以上のように第25の発明では、センタ
部または中継装置が第二のワーク鍵を、秘密鍵を用い
暗号化を行い、伝送するようにしたので、第二のワー
ク鍵を安全に共有することができるという効果が得られ
る。

【0069】第26の発明では、センタ装置または中継装置は第二のワーク領域を、公開鍵暗号方式を用いて暗号化を行い、伝送するという手段を有している。

16

(0070) 以上のように第28の発明では、センタ装置または中継装置が第二のワーク鍵を、公開鍵を用いて暗号化を行い、伝送するようにしたので、第二のワーク鍵を安全に共有することができるという効果が得られる。

〔0071〕第27の発明では、センタ装置は、必要に応じて第二の共通情報に第一の視聴履歴収集先の電話番号を格納して送出し、中継装置は、必要に応じて第二の個別情報に第二の視聴履歴収集先の電話番号を格納して送出し、端末装置は、第一の視聴履歴収集先の電話番号を優先的に使用して視聴履歴を送信するという手段を有している。

〔0072〕以上のように第27の実例では、センタ装置が必要に応じて第二の共通情報に第一の複製履歴収集先の電話番号を格納して送出し、中継装置は、必要に応じて第二の個別情報に第二の複製履歴収集先の電話番号を格納して送出し、端末装置は第一の複製履歴収集先の電話番号を優先的に使用して複製履歴を送信するようにしたで、任意の複製履歴収集先で複製履歴を収集することができるといった効果が得られる。

【0073】第28の発明では、共通情報除去装置は中継装置に設置され、コンテンツを含む情報から第一の共通情報を取り除くという手段を有している。

【0074】以上のように第28の発明では、共通情報除去装置が、コンテンツを含む情報から第一の共通情報を取り除くようにしたので、第二の伝送路上に第二の端末装置には不要な第一の共通情報がなくなるので、第二の端末装置の動作を簡便にするという効果が得られ

【0075】第28の発明では、共通情報多重装置は中継装置に設置され、第一の伝送路から受信したコンテンツを含む情報の第一の共通情報と、第三の伝送路から受信した第二の共通情報とを入れ替えるという手段を有している。

〔0078〕以上のように第28の発明では、共通情報多量装置が、第一の伝送路から受信したコンテンツを含む情報の第一の共通情報と、第三の伝送路から受信した第二の共通情報とを入れ替えるようにしたので、第一の伝送路上のコンテンツを含む情報の伝送容量を増やすことなく第二の伝送路に中継できるという効果が見られる。

【0077】第30の発明では、個別情報除去装置は中継装置に設置され、コンテンツを含む情報から第一の個別情報を取り除くという手段を有している。

【0078】以上のように第30の発明では、個別情報除去装置が、コンテンツを含む情報から第一の個別情報を取り除くようにしたので、第二の伝送路に送出する情報の伝送容量を増加でき、第二の端末装置には不要な第一の個別情報がなくなるので、第二の端末装置の著作権防止につながるという効果が得られる。

17

【0078】第31の発明は、結合装置に設置され、コンテナの位置検知と、第二の位置検知を有している。

【0080】以上のように多重装置がコンテンツを含むと、第二の複製情報とをたので、第一の伝送路上の容量を増やすことなく第二効果が得られる。

【0081】第32の発明は、送受信機に設置され、受信した無線電波の周波数を検出し、検出した周波数に基づいて、送信機に送信する周波数を決定する手段を有している。

[0082]以上のように、多量装置が、受信した第二の第二の共通情報を受信するにしたので、第一の伝送容量を増加させることができる高品質化や、マルチチャネル。

【0083】
【発明の実施の形態】以下

て、図面を用いて説明する
 施の形態に何ら限定される
 脱しない範囲において、明
 【0084】（第1の実施例）
 は、限定受信システムの一

説明する。

【0085】図1は、本実施例の全体構成を示すブロック図である。

【0088】放送センタ
103を利用した衛星目標10
タ101と直接受信端末104
更にCATV局105とCA
6で接続される。

【0087】放送センター
出し、直接受信端末1042
信する。CATV局1052は
電波をCATV目録1050
ATV目録106から放送電

【0088】図2は放送
示すブロック図の一例で、

【0089】放送センタ
コンテンツを送出するコ
Kw (ワーク関) を保持
第二の Kw を保持する第
Kw 及び直接受信端末 10
(個別情報) に格納し、

(10)

特製2001-69480

(仮称)で暗号化する第一のECM生成部202と、一定期間でKs(スクランブル)を生成するKs生成部203と、Ks及び既定数値の対称と異なるコネクションの根拠決定情報第一のECMへ格納し、第一のKwを用いて暗号化する第一のECM生成部204と、Ks及び既定数値の対称と異なるコネクションの根拠決定情報第二のECMへ格納し、第二のKwを用いて暗号化する第二のECM生成部205と、Ksを第一のECM生成部204及び第二のECM生成部205へ共通渡し、Ks及びスクランブル

の対象となるコンテナのバケット識別子 (PID) を
 スキャンする210へ送信し、第一のECMを生成する202及び
 第二のECMを生成する204から入力する第一のECM及び
 第二のECMを多重部209へ送達するタイムマルチプレ
 キング制御部207と、コンテナ、第一のECM、第一のEC
 M及び第二のECMを多重してトランスポートストリー
 ムとして出力する多重部208と、トランスポートストリー
 ム内のコンテナのバケットをKsを用いてスキャン
 するスキャン部210と、画像記録102Cに記憶したデータ
 などの処理を行う送達部212と、変調回路102へトランス
 ポートストリームを放送電波として送達する送達アン
 テナ213とを備える。

【0090】コンテンツサーバ201はMPEG2規格の
 トランスポートストリーム形式で、映像や音声などを含
 むコンテンツを多量に209へ送信する。第一のKw管理
 部203は第一のKwを保持しており、第一のEMM生成
 部202及び第一のECM生成部204へ第一のKwを送信
 し、第一のEMM生成部202は第一のKw及び直接受信
 した104の契約情報と第一のEMMに格納し、この直接
 受信した契約情報とKmi(個別鍵)で、第一のEMM

の暗号化すべき領域を暗号化し、多量部209へ送信する。第二のKw管理部206は第二のKwを保持し、第二のECM生成部205へ第二のKwを送信し、Ks生成部207へ送信する。

008は一定間隔でKsを生成し、サイマルクリプト制御部207へ送信する。サイマルクリプト制御部207はKsを第一のECM生成部204及び第二のECM生成部2050それぞれへ送信し、第一のECM生成部204は、Ks及び限定受信の対象となるコンテンツの複製判定情報を第一の

ECMへ格納し、第一のKwを用いて、第一のECMの暗号化すべき領域を暗号化してサイマルクリプト暗号データを送信する。第二のECM生成部は、Ks及び第一のECMを受信の対象となるコンテンツの複製判定情報と第二のECMへ格納し、第二のKwを用いて、第二のECMの暗号化すべき領域を暗号化してサイマルクリプト暗号データを生成する。

207へ送信する。サイマルクリプト制御部207は、K及びスクランブルの対象となるコンテンツのパケット識別子(PID)をスクランブラ210へ送信し、第一のECM及び第二のECMを多重部209へ送信する。多重部209は、受信したコンテンツ、第一のECM、第一のECM及び第二のECMを多重して1つのトランスポートストリームとしてスクランブラ210へ送信する。スクラン

•

22

局の内部構成図。

(図28) 本発明の第7の実施の形態におけるCATV局以上の放送帯域を示す図。

(図29) 本発明の第7の実施の形態におけるCATV局の内部構成図。

(図30) 本発明の第8の実施の形態におけるCATV局の内部構成図。

(図31) 本発明の第8の実施の形態におけるCATV局の内部構成図。

(図32) 本発明の第9の実施の形態における放送センタの内部構成図。

(図33) 本発明の第9の実施の形態におけるCATV局の多重部の内部及び応答の構成図。

(図34) 本発明の第9の実施の形態における共通情報多重装置の動作を示す図。

(図35) 本発明の第10の実施の形態における放送受信システムの全体構成図。

(図36) 本発明の第10の実施の形態におけるCATV局の内部構成図。

(図37) 本発明の第11の実施の形態における放送受信システムの全体構成図。

(図38) 本発明の第11の実施の形態における放送センタの内部構成図。

(図39) 本発明の第11の実施の形態における第二のCATV局の内部構成図。

(図40) 従来のバスルー一方式を説明する図。

(図41) 従来のサイマルクリップ方式を説明する図である。

【符号の説明】

101、3703 放送センタ

104、3702 放送受信端末

105 CATV局

107 CATV局

202、3803 第一のEMM生成部

304、3804 第一のECM生成部

*205、3002、3806 第二のECM生成部

206、3001、3805 第二のKw管理部

207、3003、3809 サイマルクリップ制御部

303、2703、3903 PSI変換部

304、3904 多重部

305、2704、3905 QAM変換部

306、2705、3906 周波数変換部

307、2706、3001 第二のKw管理部

308、2707、3002 第二のEMM生成部

404、504、2904、3104 分離部

405、505、2905、3105 既定受信スケジュール

1301 共通情報除去装置

1302、1302、2302、3302 多重装置

1501 ECM抽出子

1501 抽出情報多重装置

1701 ECM抽出子

1901 抽出情報多重装置

2301、3301 共通情報多重装置

2302 番組属性

2710 変換部

2710 周波数変換部

2902 分配器

2909 第一のEMM抽出部

3003 送信部

3101 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

3104 送信部

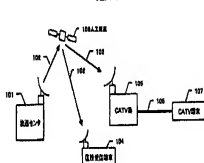
3104 送信部

3104 送信部

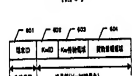
3104 送信部

3104 送信部

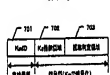
(図1)



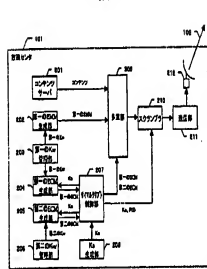
(図6)



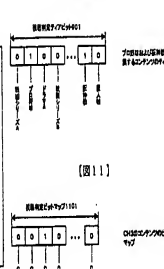
(図7)



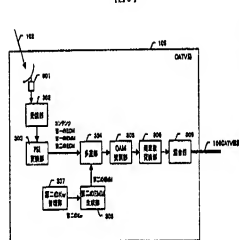
(図2)



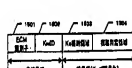
(図9)



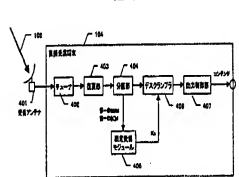
(図3)



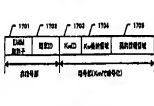
(図15)



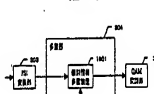
(図4)



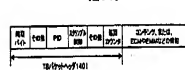
(図17)



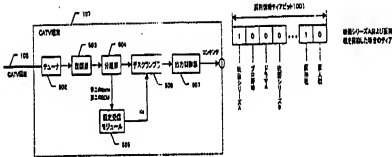
(図18)



(図14)



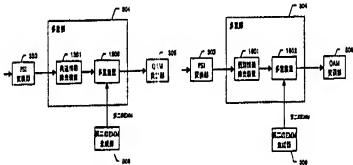
(図5)



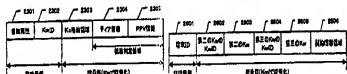
(図8)



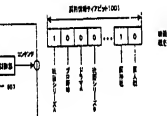
(図13)



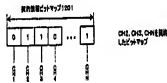
(図23)



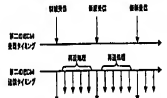
(図10)



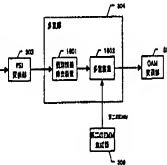
(図12)



(図22)



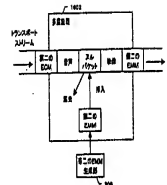
(図18)



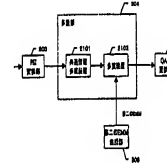
(図26)



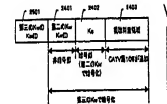
(図18)



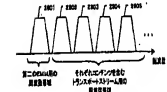
(図21)



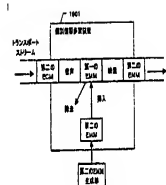
(図25)



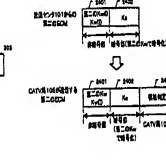
(図28)



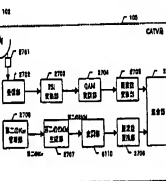
(図20)



(図24)



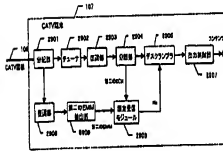
(図27)



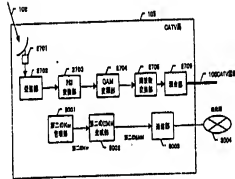
(27)

特開2001-59480

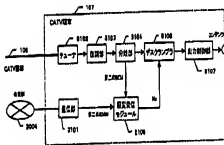
【図29】



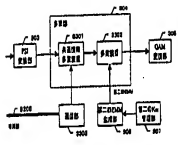
【図30】



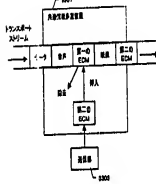
【図31】



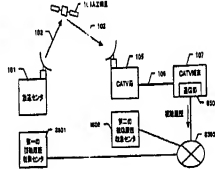
【図33】



【図34】



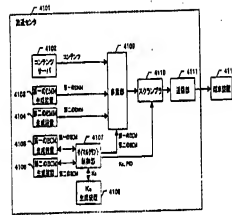
【図35】



(30)

特開2001-89480

【図41】



フロントページの続き

- (72)発明者 櫻井 博典
大阪府門真市大字門真100番地 松下電器
産業株式会社内
- (72)発明者 内藤 英文
大阪府門真市大字門真100番地 松下電器
産業株式会社内
- (72)発明者 後藤 吉正
大阪府門真市大字門真100番地 松下電器
産業株式会社内
- Fターム(参考) 5C064 C041 C001 C002 C004
S1104 A021 A016 B002 B003 E004
E005 E017 J003 N003 P004
P005